[redacted]

U.S. Department of Justice
United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

January 31, 2020

By Hand
The Honorable Paul A. Crotty
United States District Judge
Southern District of New York
United States Courthouse
500 Pearl Street
New York, New York 10007

Re: United States v. Joshua Adam Schulte, S2 17 Cr. 548 (PAC)

Dear Judge Crotty:

[redacted]We write in connection with the Court's order, dated January 30, 2020 (the "Order"), in which the Court directed the Government to explain how it intended to use the information downloaded from the WikiLeaks website (the "WikiLeaks Information") at trial, and to explain how the Government's proposal accords with the four-factor test for courtroom closures set forth in *Waller v. Georgia*, 467 U.S. 39, 46 (1984). As the Court noted, Section 8 of the Classified Information Procedures Act ("CIPA") permits the Government to enter material into evidence without changing its classification status. As set forth in the Government's motion pursuant to Section 6 of CIPA, the Government intends to invoke Section 8 with respect to the WikiLeaks Information and one voluminous log file (which was not publicly disclosed by WikiLeaks) (the "Log File").

[redacted]*First*, with respect to how the Government intends to introduce and present the WikiLeaks Information at trial, the Government plans to introduce both a classified version of the entirety of the WikiLeaks Information, which includes the CIA leaked information (the "Leaked Information") and excerpts of the Leaked Information (the "Excerpts") which have been declassified for use at trial. At trial, a special agent with the Federal Bureau of Investigation (the "FBI") will testify that he visited the WikiLeaks website and downloaded the WikiLeaks Information onto a standalone laptop (the "Laptop"), which will be marked as a Government exhibit. The special agent will also testify that, because the Leaked Information within the WikiLeaks Information remains classified, he was required by regulation to follow certain special procedures to download it, including not downloading it in an FBI work space or onto a networked computer, and storing the Laptop in a manner that is consistent with protecting classified information. The special agent will also testify that he extracted the Excerpts from the Leaked Information. The Government will then introduce the Laptop and the WikiLeaks Information into evidence as a classified exhibit (which could be viewed by the jury, the parties, and the Court), and the Excerpts as unclassified exhibits. The Government will also adopt the same approach with the Log File—while the Government will introduce the Log File as a whole

[redacted]

[redacted]

as a classified exhibit, it will introduce relevant portions of the Log File as unclassified selections (the "Log File Selections").

[redacted] The Government does not intend to publicly display the WikiLeaks Information or the Log File during trial. For all of the reasons set forth further below, publicly displaying the contents of the WikiLeaks information would increase the risk that such materials pose to the public and harm the national security. Moreover, given the sheer volume of the WikiLeaks Information and the Log File, which includes thousands of pages, it would simply be impractical to display the WikiLeaks Information or the Log File publicly page by page, even setting aside the classification issues and the danger to the public. Instead, as is often the case with particularly voluminous exhibits, the Government will display publicly the Excerpts and the Log File Selections. The Government will publicly display the declassified Excerpts and the Log File Selections during, for example, the testimony of CIA witnesses who worked on the classified CIA tools described in the Excerpts or who administered DEVLAN. These witnesses will explain generally what these tools were (*i.e.*, that they were developed to gather intelligence from foreign targets), how these witnesses kept information about these tools closely held, and why they did so. This evidence is directly relevant to an element of several of the charged offenses, specifically, that the information the defendant illegally gathered and transmitted to WikiLeaks was national defense information. Similarly, the unclassified Log File Selections are evidence of activity on the relevant portions of DEVLAN, including the defendant's deletion of log files showing his activity on the network on April 18 and 20, 2016.

[redacted] Some of these witnesses will also testify about the Leaked Information based on their review of the entirety of the WikiLeaks Information prior to the testimony. While the Court already has authorized the partial closure of the courtroom during the testimony of these witnesses in response to the Government's witness protection motion, the Government is not seeking any additional closure based on the fact that this portion of their testimony concerns the entirety of the Leaked Information—in other words, the public will be able to hear this testimony unimpeded. That testimony is relevant to several issues at trial. For example, these witnesses will testify about the massive amount of sensitive information that is included in the Leaked Information, which helps to show, among other things, that the defendant intended to or had reason to believe that the Leaked Information could be used to injure the United States, which are elements of the various espionage counts with which the defendant is charged. *See* 18 U.S.C. §§ 793(b) (requiring an intent to harm the United States or benefit a foreign nation) & (d)-(e) (requiring, in some cases, that the defendant had reason to believe that the transmission of the national defense information could harm the United States or benefit another country). Similarly, the full scope of the Leaked Information also helps to explain where it came from—if the jury was led to believe that WikiLeaks had only disclosed a few documents, then it may believe (incorrectly) that the Leaked Information could have been taken from an individual user's CIA workstation, for example. Moreover, as the Court is aware, the defendant wrote in his prison notebooks that WikiLeaks had source code for a specific tool—a review of the Leaked Information, however, shows that there is no such source code there. As explained in prior submissions, this evidence helps to demonstrate that the defendant was the perpetrator of the crime, because he knows non-public information about what WikiLeaks possesses.

[redacted] *Second*, the Government respectfully submits that this treatment of the Leaked Information is appropriate under *Waller*. Under *Waller*, there are four factors the Court must

[redacted]

[redacted]

consider: (1) the party seeking the limitation advances an overriding interest that is likely to be prejudiced; (2) the limitation is no broader than necessary; (3) the court considers reasonable alternatives; and (4) the court makes findings adequate to support the limitation. 467 U.S. at 48. *United States v. Alcantara*, 396 F.3d 189, 199-200 (2d Cir. 2005) (setting forth procedural protections generally applicable to closure motions). "The same test applies whether a closure motion is made by the government over the defendant's Sixth Amendment objection or made by the defendant over the First Amendment objection of the government or press." *United States v. Doe*, 63 F.3d 121, 128 (2d Cir. 1995).

[redacted] With respect to the first *Waller* factor, there is an "overriding" interest in protecting the Leaked Information and the Log File from unnecessary public exposure. The unlawful dissemination of the classified information in the Leaked Information does not strip that information of its classification. *See* Executive Order 12356, § 1.3(a) (classified information "shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure"). Indeed, permitting such a result would incentivize the unauthorized leaking of classified information by giving the leaker final say over whether information should be classified, rather than the officials tasked with evaluating the totality of circumstances in determining whether disclosure of the information would harm the nation's security. *See El-Masri v. United States*, 479 F.3d 296, 305 (4th Cir. 2007) ("The executive branch's expertise in predicting the potential consequences of intelligence disclosures is particularly important given the sophisticated nature of modern intelligence analysis, in which the significance of one item of information may frequently depend upon knowledge of many other items of information, and what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.") (citation and quotations omitted)). Thus, requiring the Government to strip the protections of classification from leaked information for the purposes of prosecution would put the Government in the untenable position of having to choose between protecting national security information disclosed by leakers and prosecuting individuals, such as the defendant, who nevertheless choose to disclose that sensitive information unlawfully. CIPA's protections were expressly intended to protect against such a result. *See United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996) (CIPA's fundamental purpose is to "harmonize a defendant's right to obtain and present exculpatory material upon his trial and the government's right to protect classified material in the national interest") (internal quotation marks omitted). Section 8 furthers this goal by allowing the Government to enter classified information into evidence without declassifying it. 18 U.S.C. App. 3 § 8(a) ("Writings, recordings, and photographs containing classified information may be admitted into evidence without changing their classification status.").

[redacted] The fact that the Leaked Information has been publicly released does not mitigate either the harm sought to be avoided or the need to maintain this information in its classified state. Although in different circumstances, the Second Circuit has recognized precisely this type of harm when authorizing the restriction from public view of trial exhibits in a case involving child pornography, noting that the restriction was authorized to limit the "continuing harm to victims of child pornography." *United States v. Killingbeck*, 616 F. App'x 14, 16 (2d Cir. 2015). Those principles hold true here as well—repeated dissemination of offensive cyber-tools that would allow, among other things, the targeting of Americans by malignant actors only exacerbates the harm caused by the original leak. Indeed, the tools contained in the release remain dangerous cyber tools today, with

[redacted]

[redacted]

many computer systems and networks still vulnerable to exploitation by the very tools at risk of further disclosure here.[1] Moreover, forcing the Government to, in effect, condone and perpetuate the harm caused by the leak by releasing this information to the public in the context of a criminal trial would encourage other bad actors to leak classified information, knowing that in doing so, they may escape prosecution because the Government cannot accept indiscriminate public disclosure and acknowledgement of the leaked classified material. Thus, even though the Leaked Information is available online, there is still good reason for the Government to maintain its classification and seek to restrict unnecessary dissemination of that material wherever possible.

[redacted] It is indisputable that the Government has an "overriding" interest in protecting classified information from disclosure to unauthorized individuals. *See Dept. of Navy v. Egan*, 484 U.S. 518, 527 (1988) (government has "compelling interest" in withholding national security information from unauthorized persons). A critical component of this protection is withholding classified information from those who without a genuine "need-to-know." *See* Executive Order 12,958 § 4.2(a)(3) (restricting circumstances in which person may receive classified information to when "the person has a need-to-know the information"). To be sure, the Government does not deny that the public has an interest in learning what caused the disclosure of the Leaked Information, and, indeed, through this trial, the jury and the people are going to receive an unprecedented window into the workings of a clandestine intelligence agency. But absent a specific showing that the public has a reason to know every shred of information in the Leaked Information or the Log File, there is simply no reason to disclose all of this classified information to the public.[2]

[redacted] Moreover, with respect to the second and third *Waller* factors—the need for the restriction to be as limited as possible and the absence of any reasonable alternatives, *see* 467 U.S. at 48—the Government's approach is appropriate. Initially, the defense and the jury are not being denied any information—they will have full access to the WikiLeaks Information on the Laptop. The public will also gain an understanding of the kinds of information that is in the Leaked Information through the declassified Excerpts, which are substantive documents like user guides and source code for CIA cyber-tools, and witness testimony about the Leaked Information. The only thing the public

---

[1] (U) The CIA is prepared to provide a more detailed declaration, on an *ex parte* basis, if the Court requires further detail regarding the continuing danger of these tools and the harm associated with repeated disclosure.

[2] (U) Indeed, the Government notes that, as this Court did, courts in this District have routinely approved of withholding classified CIPA Section 4 motions from cleared defense counsel involved in those prosecutions when those attorneys did not have a need to know the classified information the Government sought to delete. *See, e.g.*, *United States v. Zarrab*, 15 Cr. 867 (RMB) (2017); *United States v. Pham*, No. 12 Cr. 423 (AJN) (2015); *United States v. al Liby*, S10 98 Cr. 1023 (LAK) (2014); *United States v. Abu Ghayth*, S13 98 Cr. 1023 (LAK) (2014); *United States v. al Fawwaz & Abdel Bary*, S7 98 Cr. 1023 (LAK) (2013); *United States v. Mustafa*, 04 Cr. 356 (KBP) (2013); *United States v. Chichakli*, 09 Cr. 1002 (WHP) (2013); *United States v. El-Hanafi*, S5 10 Cr. 162 (KMW) (2012); *United States v. Ghailani*, S10 98 Cr. 1023 (LAK) (2010); *United States v. al-Kassar*, 07 Cr. 354 (JSR) (2009); *United States v. Kassir*, S2 04 Cr. 356 (JFK) (2008); *United States v. Wadih el Hage, et al.*, S7 98 Cr. 1023 (LBS) (2000).

[redacted]

[redacted]

will not be able to do is browse with Government imprimatur through the voluminous material in the Leaked Information about dangerous cyber-tools. Similarly, the public will receive all of the information from the Log File Selections about what actually happened on DEVLAN during the relevant time periods, including the defendant's deletion of log files to conceal his activity, without learning details of a voluminous amount of unrelated network activity. There is no way to avoid the harms that could result from public disclosure, however, short of restricting the Leaked Information from the public.

[redacted] Finally, as to the final *Waller* factor, the Court has ample basis upon which to make factual findings necessary to support granting the Government's proposal. In connection with the Government's application, the Government submitted a 52-page Declaration [redacted] specifically addresses the national security reasons supporting the Government's approach. [redacted]

(U) The Government respectfully submits that, in light of the foregoing, the Government's proposal for use of the WikiLeaks Information and the Log File is appropriate.

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By: /s/
David W. Denton Jr. / Sidhardha Kamaraju /
Matthew Laroche
Assistant United States Attorneys
(212) 637-2744 / 6523 / 2420

[3] (U) Although the defendant has given generalized notice pursuant to Section 5 of CIPA that he intends to introduce the entirety of the Wikileaks Information, he never given notice that is "particularized, setting forth specifically the classified information which the defendant reasonably believes to be necessary to his defense." *United States* v. *Collins*, 720 F.2d 1195, 1199 (11th Cir. 1983).

[redacted]